

REMARKS

The claimed invention as described in one of the embodiments of the disclosed invention is a data sending/receiving device and digital certificate issuing method in which a network consists of a plurality of data sending/receiving devices. The claimed invention may allow additional data sending/receiving devices to simply be added to the network **without** their pre-authorization, simplifying many approaches to network configuration and modification.

Claims 1-15 are pending in the present application. Claims 1-9, 11-13 and 15 have been amended as a result of this response. No claims have been added or canceled. Applicants respectfully submit that independent claims 1, 4, 7, 11 and 15 and dependent claims 2-3, 5-6, 8-10 and 12-14 stand in condition for allowance.

I. 35 U.S.C. 132(a) Objections

The Examiner has objected to the amendment filed on March 17, 2008 under 35 U.S.C. 132(a) because it allegedly is not supported by the disclosure. Specifically, the Office Action objects to claims 1 and 4 for reciting “a control section which performs a dynamic process of issuing the digital certificate” and claim 15 for reciting, “performing a dynamic process of issuing the digital certificate.”

Claims 1, 4 and 15 have been amended to remove “dynamic” from the claim. Applicants respectfully request withdrawal of the objection.

II. Claim Rejections Under 35 U.S.C. § 103(a)

The Examiner has rejected claims 1-14 under 35 U.S.C. § 103(a) as being unpatentable over Balfanz et al. (U.S. 2003/0149874 A1) in view of Hind et al. (U.S. Pat. No. 6,772,331 B1) and in further view of Vilhuber (U.S. 7,386,721 B1). These rejections are respectfully traversed.

Balfanz

Balfanz discloses a system for authenticating a communication between at least two devices that is transmitted using a network medium after the network has already been established ([0002]). Balfanz is significantly different from the claimed invention in that the different embodiments of Balfanz utilize a network already in place, which require a complex set-up **before** it can authenticate communications based on pre-authentication information.

Balfanz merely describes the authentication of communications including describing a number of different hand-shakes or multiple information exchanges between network devices for authenticating communication between pre-established, designated and pre-authenticated network devices. For example, “a first network device sends pre-authentication information to a second device over a location-limited channel...[a] second device responds by sending its pre-authentication information to the first device over the location-limited channel” (paragraph [0015]). The first and second devices in the prior example both already have pre-authentication information, which allow it to participate in the network and Balfanz is merely describing the way in which a secure communication can be made with the participating devices on the network. When a device in the network is a group manager, the group manager may disseminate the exchange of the pre-authentication information with the remaining devices, to restate, the manager may speed up the authentication process of an already designated network device to the rest of the group (paragraph [0017]).

In Balfanz, it is also possible that a new device can be added to the secure communication, this new device would be required to have already received pre-authorization to communicate within the network. However, since the device is new to the current group of participants (for example came within range, or was turned on), the new device communicates with the group manager exchanging pre-authentication information before the new device can actively communicate within the network (paragraphs [0067] – [0068]). The group manager in turn disseminates the exchange of the pre-authentication information with the remaining devices (paragraph [0068]). The group manager may also disseminate a shared group key to further encrypt communications within the group.

Balfanz fails to disclose or suggest the processes of adding a device that is *not* part of the network and that has *not* already been pre-authorized. Balfanz also fails to disclose or suggest issuing a digital certificate through a secure communication to a device that is not part of the network.

Hind

Hind discloses a method and apparatus for authentication, securely generating and exchanging cryptographic keys for encryption (Column 6, lines 10-25). Hind is significantly different from the claimed invention in that the different embodiments of Hind utilize a network already in place, which required a complex set-up **before** it can authenticate communications based on unique identifiers. Specifically, the administration server or initializing device sends an inquiry to the new mobile device requesting mobile device's unique identifier and the mobile device transmits its unique identifier to the administration server (Column 9, lines 16-20). The administrator at the administration server then verifies that the unique identifier transmitted by the mobile device is the same as that received regarding that device by another means such as printed on the device (manual check) or in the device documentation (manual check), etc. (Column 9, lines 20-32). In addition, the administrator enters a PIN or encryption key on one or both of the administration server and mobile device such that a temporary secure link can be established for the purpose of device initialization before the device is allowed to participate in the established network (Column 9, lines 26-30). Restated, a device must be manually approved by an administrator or pre-authenticated before it can participate in the network.

The administration server may request that a certificate is prepared for the mobile device by the Certificate Authority before the mobile device can participate in the network (Column 9, lines 37-49). However, Hind does not disclose a dynamic process of issuing a digital certificate to a new device when the new device is connected to a managing device in the network. Rather Hind discloses a manual process requiring a person to authenticate a device before a certificate can be requested.

Vilhuber

Vilhuber discloses a method and apparatus for integrated provisioning of an network device. Vilhuber does not remedy the noted deficiencies of Balfanz and Hind. Therefore, the asserted combination of Balfanz and Hind and in further view of Vilhuber (assuming these references may be combined, which Applicants do not admit) fails to establish prima facie obviousness of any pending claim.

Discussion

Balfanz and Hind both fail to disclose or suggest a data sending/receiving device and digital certificate issuing method in which a network consists of a plurality of data sending/receiving devices and may allow additional data sending/receiving devices to simply be added to the network. Specifically, Balfanz and Hind both fail to disclose or suggest “a second communication section, to which the new data sending/receiving device can be connected by a wired connection means” and “a control section which performs a process of issuing the digital certificate for the new data sending/receiving device through the wired connection means” (claim 1). Also, Balfanz and Hind both fail to disclose “when the new data sending/receiving device is connected to the second communication section, the control section judges whether or not the new data sending/receiving device is a device having a communication means that can communicate in the wireless network, in accordance with device type information of the new data sending/receiving device received via the second communication section from the new data sending/receiving device” (claim 1). Also, Balfanz and Hind both fail to disclose “if the new data sending/receiving device is judged as a device having the communication means that can communicate in the wireless network, the control section creates the digital certificate for the new data sending/receiving device by using a device identifier specific to the new data sending/receiving device, the device identifier being received via the second communication section from the new data sending/receiving device through the wired connection means, and sends the created digital certificate via the second communication section to the new data sending/receiving device through the wired connection means” (claims 1).

Balfanz and Hind also both fail to disclose “when the new data sending/receiving device is connected to a second communication section of said another data sending/receiving device by a wired connection means, the control section of said data sending/receiving device judges whether or not the new data sending/receiving device is a device having a communication means that can communicate in the wireless network, in accordance with device type information of the new data sending/receiving device

received via a second communication section of said another data sending/receiving device through the wired connection means from the new data sending/receiving device” and “if the new data sending/receiving device is judged as a device having a communication means that can communicate in the wireless network, the control section of said data sending/receiving device creates a digital certificate for the new data sending/receiving device by using a device identifier specific to the new data sending/receiving device, the device identifier being received through the wired connection means via said another data sending/receiving device to which the new data sending/receiving device is connected from the new data sending/receiving device, and controls to send the created digital certificate through the wired connection means via said another data sending/receiving device to which the new data sending/receiving device is connected” (claim 4).

Balfanz and Hind both fail to disclose or suggest a method or program for “connecting the new data sending/receiving device through a wired connection means to” a certain “data sending/receiving device participating in the wireless network” (claims 7 and 11). Also, Balfanz and Hind both fail to disclose or suggest a method of judging by a certain data sending/receiving device, “whether or not the new data sending/receiving device is a device having a communication means that can communicate in the wireless network in accordance with device type information of the new data sending/receiving device received through the wired connection means from the new data sending/receiving device” (claims 7, 11 and 15).

Also, Balfanz and Hind both fail to disclose or suggest a method where “if the new data sending/receiving device is judged as being a device having a communication means that can communicate in the wireless network, creating a digital certificate for the new data sending/receiving device by using a device identifier specific to the new data sending/receiving device received from the new data sending/receiving device through the wired connection means and sending the created digital certificate to the new data sending/receiving device through the wired connection means, by the certain data sending/receiving device” or a method where “if the first data sending/receiving device,

which is other than the second data sending/receiving device to which the new data sending/receiving device is connected through the wired connection means, judges that the new data sending/receiving device is judged as being a device having a communication means that can communicate in the wireless network, creating a digital certificate for the new data sending/receiving device by using a device identifier specific to the new data sending/receiving device received via the second data sending/receiving device, to which the new data sending/receiving device is connected through the wired connection means, from the new data sending/receiving device and sending the created digital certificate via the second data sending/receiving device, to which the new data sending/receiving device is connected through the wired connection means, to the new data sending/receiving device, by the first data sending/receiving device" (claims 7 and 11). In addition, Balfanz and Hind both fail to disclose or suggest a computer program when executed causes a processor to execute step of "if the new data sending/receiving device is judged as being a device having a communication means that can communicate in the wireless network, creating a digital certificate for the new data sending/receiving device by using a device identifier specific to the new data sending/receiving device received from the new data sending/receiving device through the wired connection means and sending the created digital certificate through the wired connection means to the new data sending/receiving device, by the certain data sending/receiving device" (claim 15).

Accordingly, for at least these reasons, claims 1, 4, 7, 11 and 15 are clearly distinguishable over Balfanz et al. in view of Hind et al. and in further view of Vilhuber. Applicants submit that claims 2-3, 5-6, 8-10 and 12-14 are allowable at least by virtue of their dependency on claims 1, 4, 7 and 11. Accordingly, reconsideration and withdrawal of this rejection is respectfully requested.

III. Conclusion

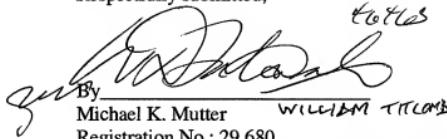
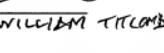
All matters having been addressed in view of the foregoing, Applicants respectfully request the entry of this Amendment, the Examiner's reconsideration of this application, and the immediate allowance of all pending claims.

Applicants' undersigned representative remains ready to assist the Examiner in any way to facilitate and expedite the prosecution of this matter. If any point remains an issue in which the Examiner feels would be best resolved through a personal or telephone interview, please contact the undersigned at the telephone number listed below.

Please charge any fees associated with the submission of this paper to Deposit Account No. 02-2448. The Commissioner for Patents is also authorized to credit any overpayments to the above-referenced deposit account.

Dated: October 10, 2008

Respectfully submitted,


By 
Michael K. Mutter WILLIAM TITCOMB
Registration No.: 29,680
BIRCH, STEWART, KOLASCH & BIRCH, LLP
8110 Gatehouse Road
Suite 100 East
P.O. Box 747
Falls Church, Virginia 22040-0747
(703) 205-8000
Attorney for Applicant